Air Live®
Powered by OvisLink Corp.

BT-302USB

Bluetooth 3.0 Mini USB Dongle

User's Manual

www.airlive.com

Copyright & Disclaimer

No part of this publication may be reproduced in any form or by any means, whether electronic, mechanical, photocopying, or recording without the written consent of OvisLink Corp.

OvisLink Corp. has made the best effort to ensure the accuracy of the information in this user's guide. However, we are not liable for the inaccuracies or errors in this guide. Please use with caution. All information is subject to change without notice

All Trademarks are properties of their respective holders.

© 2009 OvisLink Corporation, All Rights Reserved

Federal Communication Commission
Interference Statement

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio technician for help.

FCC Caution

This device and its antenna must not be co-located or operating in conjunction with any other antenna or transmitter.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Any changes or modifications not expressly approved by the party responsible for compliance could void the authority to operate equipment.

Federal Communication Commission (FCC) Radiation Exposure Statement

This EUT is compliance with SAR for general population/uncontrolled exposure limits in ANSI/IEEE C95.1-1999 and had been tested in accordance with the measurement methods and procedures specified in OET Bulletin 65 Supplement C.

R&TTE Compliance Statement

This equipment complies with all the requirements of DIRECTIVE 1999/5/EC OF THE EUROPEAN PARLIAMENT AND THE COUNCIL of March 9, 1999 on radio equipment and telecommunication terminal Equipment and the mutual recognition of their conformity (R&TTE)
The R&TTE Directive repeals and replaces in the directive 98/13/EEC (Telecommunications Terminal Equipment and Satellite Earth Station Equipment) As of April 8, 2000.

Safety

This equipment is designed with the utmost care for the safety of those who install and use it. However, special attention must be paid to the dangers of electric shock and static electricity when working with electrical equipment. All guidelines of this and of the computer manufacture must therefore be allowed at all times to ensure the safe use of the equipment.

EU Countries Intended for Use

The ETSI version of this device is intended for home and office use in Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, the Netherlands, Portugal, Spain, Sweden, and the United Kingdom.

The ETSI version of this device is also authorized for use in EFTA member states: Iceland, Liechtenstein, Norway, and Switzerland.

EU Countries Not intended for use

None.

The specification is subject to change without notice.

Table of Contents

1. Introduction 1
1.1. System Requirements 2
1.2. Package Contents 2
1.3. Hardware Installation 3
2. Software Installation 4
2.1. Configuration Utility 14
2.2. Bluetooth Configuration - General 19
2.3. Bluetooth Configuration - Accessibility 20
2.4. Bluetooth Configuration – PIM Interface 22
2.5. Bluetooth Configuration - Share 24
2.6. Bluetooth Configuration – Communications Port 26
2.7. Bluetooth Configuration – Networking 27
2.8. Bluetooth Configuration - Diagnostics 28
3. Specifications 29
4. Wireless Network Glossary 30

1 Introduction

Thank you for purchasing the AirLive BT-302USB Bluetooth 3.0 Mini USB Dongle. This ultra-compact USB adapter supports the latest Bluetooth 3.0 standard and lets you connect your desktop computer or notebook computer to mobile phone, PDA, notebooks, printers or headsets. This handy and mini adapter allows you to create your Personal Area Network (PAN) instantly. You will soon be able to enjoy these additional features by following the instruction in this manual.

- Extremely compact design Bluetooth 3.0 USB adapter
- Universal Bluetooth connectivity for your computer
- Effectively power saving, ultra low power consumption
- Backward compatible with Bluetooth v1.2/2.0/2.1
- Supports A2DP stereo streaming, up to 3Mbps link speed

1.1. System Requirements

- USB 2.0 port & CD-ROM drive
- Windows XP/Vista/7 or Mac OS X 10.5/10.6
- At least 30MB of available disk space

Note: this device may not be able to work with USB 1.1 port

1.2. Package Contents

Before installing the adapter, please check if there's anything missing in the package, and contact your dealer of purchase to claim for missing items:

- BT-302USB
- Software CD

1.3. Hardware Installation

- USB Connector
- Link/Activity LED (Blue)

LED	Mode	Status
Link/ Activity	Steady ON	Connect to a USB port with power
	Flash	Transferring data
	Off	Adapter un-plugged

With the computer switched on, insert the BT-302USB adapter into an empty USB 2.0 port.

Caution: Never use force to insert the adapter

2 Software Installation

BEFORE INSTALLATION

Please remove any previous version of Widcomm Bluetooth software existing in your system. The remove procedures are as follows:

1. Click Start/Settings, and then select Control Panel

2. In the Control Panel window, double click Add/Remove programs icon

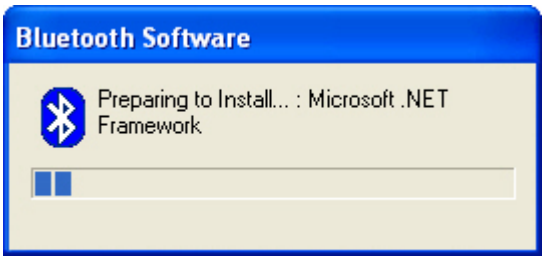
3. Find out the item Widcomm Bluetooth Software x.x.x.x then remove it

INSTALL WIDCOMM BLUETOOH SOFTWARE

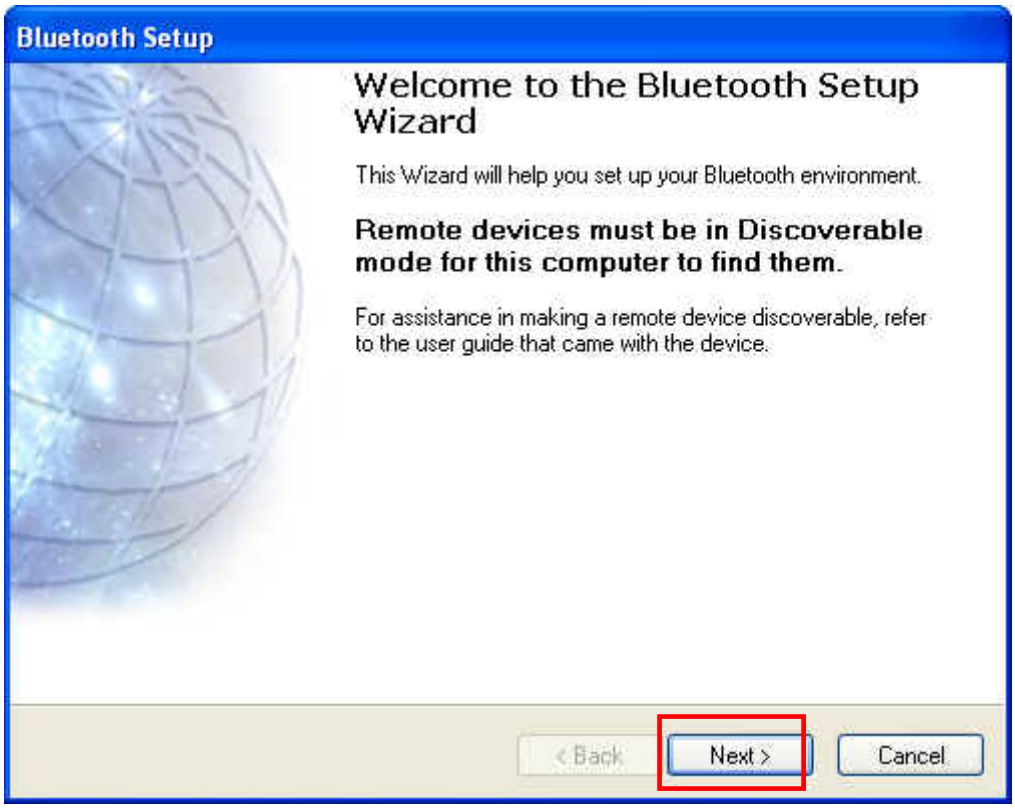
Note: The following instruction were based on Windows XP, please follow the on-screen instruction if you have different operating system.

Insert the enclosed software CD in the CDROM drive and click "**Install Driver & Utility**" from the autorun screen. If the autorun screen did not appear, run the "**Setup.exe**" program in the "**Driver**" folder.

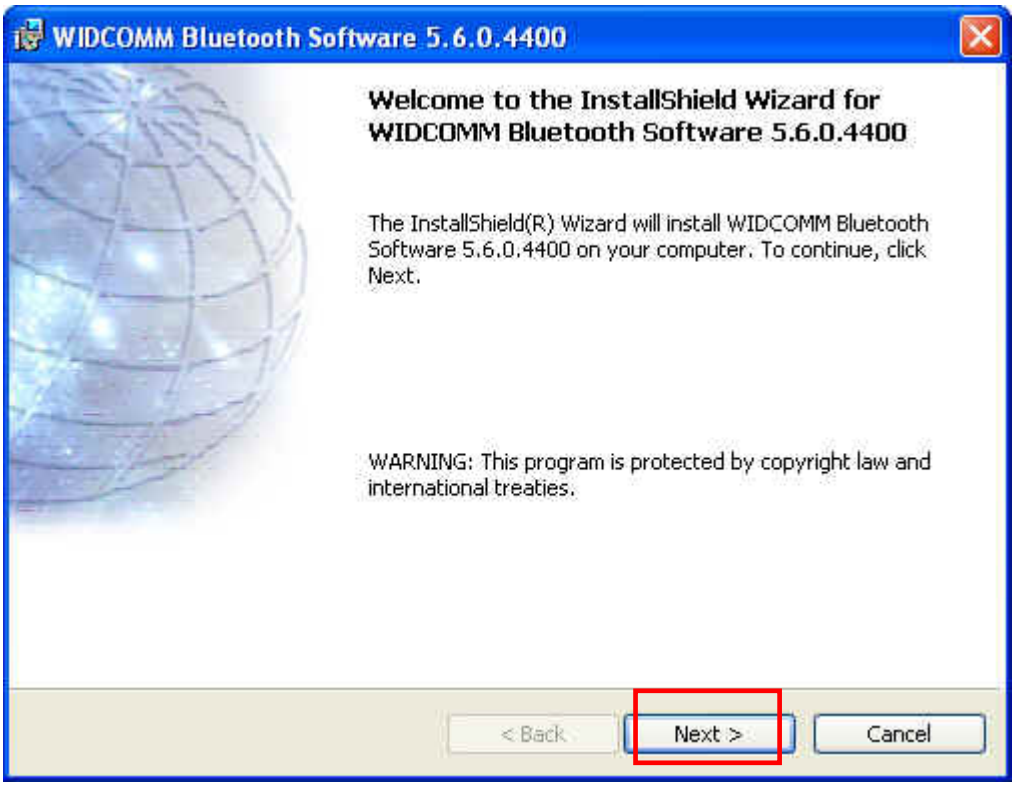
1. The system will detect and install the Microsoft Net Framework automatically.



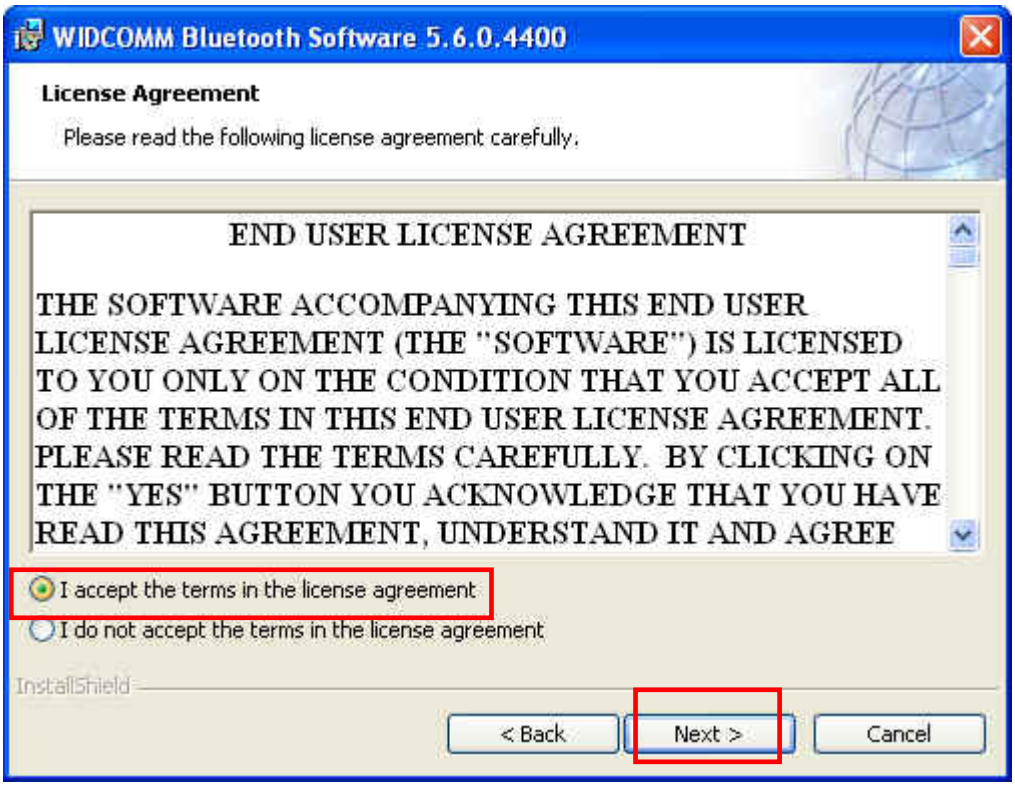
2. When the first of the Bluetooth Setup screen displays, click “Next” to continue. On any of the screens where they appear, click “Back” to return to a previous screen; click “Cancel” to exit the wizard.


Bluetooth Setup
Welcome to the Bluetooth Setup Wizard
This Wizard will help you set up your Bluetooth environment.
Remote devices must be in Discoverable mode for this computer to find them.
For assistance in making a remote device discoverable, refer to the user guide that came with the device.
< Back
Next >
Cancel

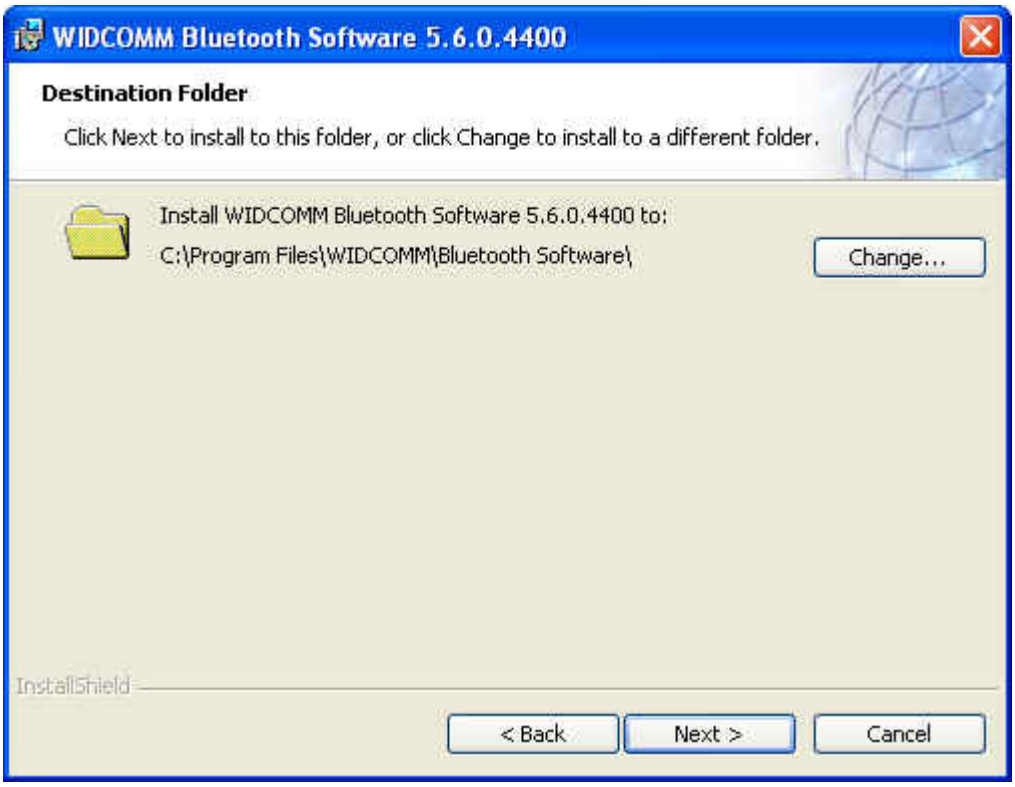
3. The Widcomm Bluetooth Software version will appear, click “Next” to continue.


WIDCOMM Bluetooth Software 5.6.0.4400
Welcome to the InstallShield Wizard for WIDCOMM Bluetooth Software 5.6.0.4400
The InstallShield(R) Wizard will install WIDCOMM Bluetooth Software 5.6.0.4400 on your computer. To continue, click Next.
WARNING: This program is protected by copyright law and international treaties.
< Back
Next >
Cancel

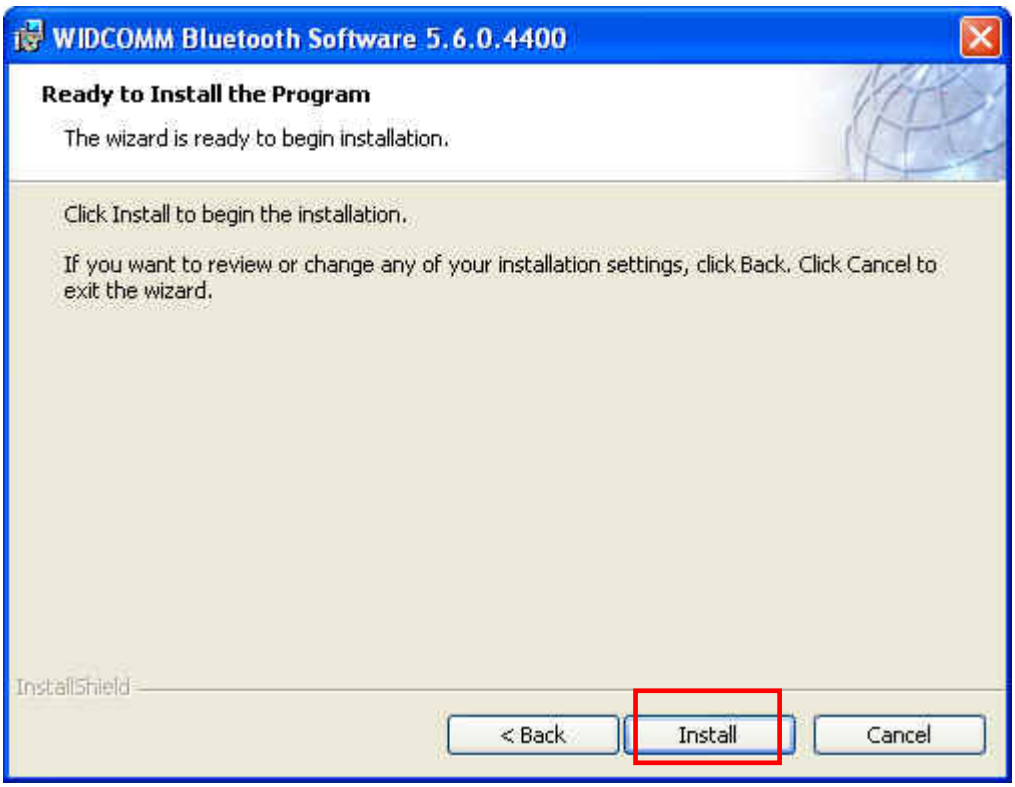
4. License Agreement screen appears, select “I accept the term in the license agreement” and click “Next.”


WIDCOMM Bluetooth Software 5.6.0.4400
License Agreement
Please read the following license agreement carefully.
END USER LICENSE AGREEMENT
THE SOFTWARE ACCOMPANYING THIS END USER LICENSE AGREEMENT (THE "SOFTWARE") IS LICENSED TO YOU ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS IN THIS END USER LICENSE AGREEMENT. PLEASE READ THE TERMS CAREFULLY. BY CLICKING ON THE "YES" BUTTON YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT, UNDERSTAND IT AND AGREE
I accept the terms in the license agreement
I do not accept the terms in the license agreement
InstallShield
< Back
Next >
Cancel

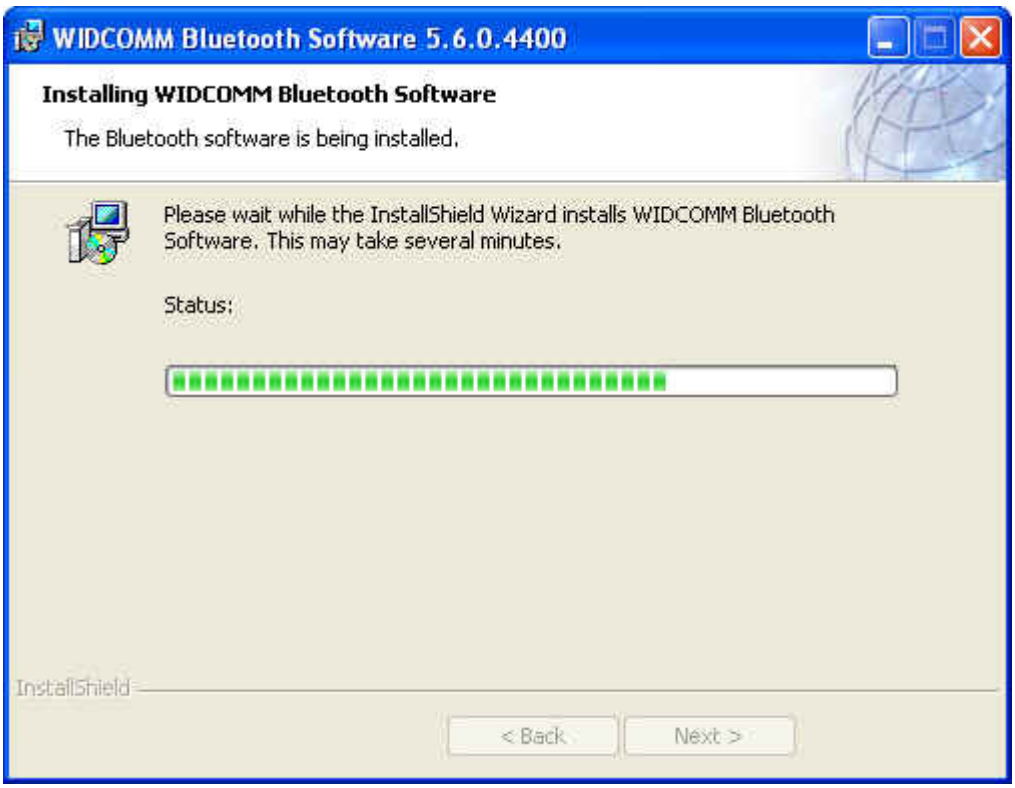
5. Click “Change” to appoint the destination of utility installation, or click “Next” to continue with default destination.


WIDCOMM Bluetooth Software 5.6.0.4400
Destination Folder
Click Next to install to this folder, or click Change to install to a different folder.
Install WIDCOMM Bluetooth Software 5.6.0.4400 to:
C:\Program Files\WIDCOMM\Bluetooth Software\
Change...
InstallShield
< Back
Next >
Cancel

6. When the next screen displays, click “Install” to begin the installation.


WIDCOMM Bluetooth Software 5.6.0.4400
Ready to Install the Program
The wizard is ready to begin installation.
Click Install to begin the installation.
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
InstallShield
< Back
Install
Cancel

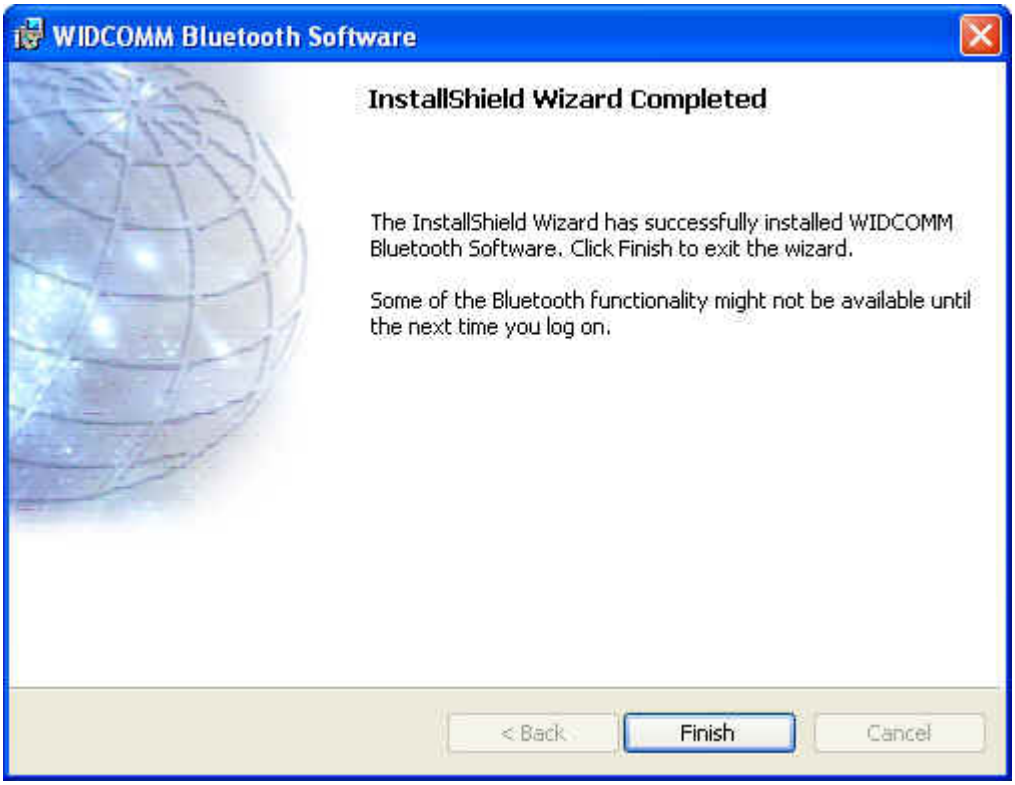
7. Please wait while the install procedure is running.


WIDCOMM Bluetooth Software 5.6.0.4400
Installing WIDCOMM Bluetooth Software
The Bluetooth software is being installed.
Please wait while the InstallShield Wizard installs WIDCOMM Bluetooth Software. This may take several minutes.
Status:
InstallShield
< Back
Next >

8. When you see this message, please follow the on-screen instruction and insert the AirLive BT-302USB into the USB port and click “OK” to continue.

Bluetooth device not found
No Bluetooth device was detected. Please make sure that your Bluetooth device is plugged in properly and click 'OK' to continue installation. Click 'Cancel' to continue installation without the Bluetooth device.
OK
Cancel

9. Click “**Finish**” to complete the driver installation process. It is recommended to restart your computer once the driver/utility installation is complete.

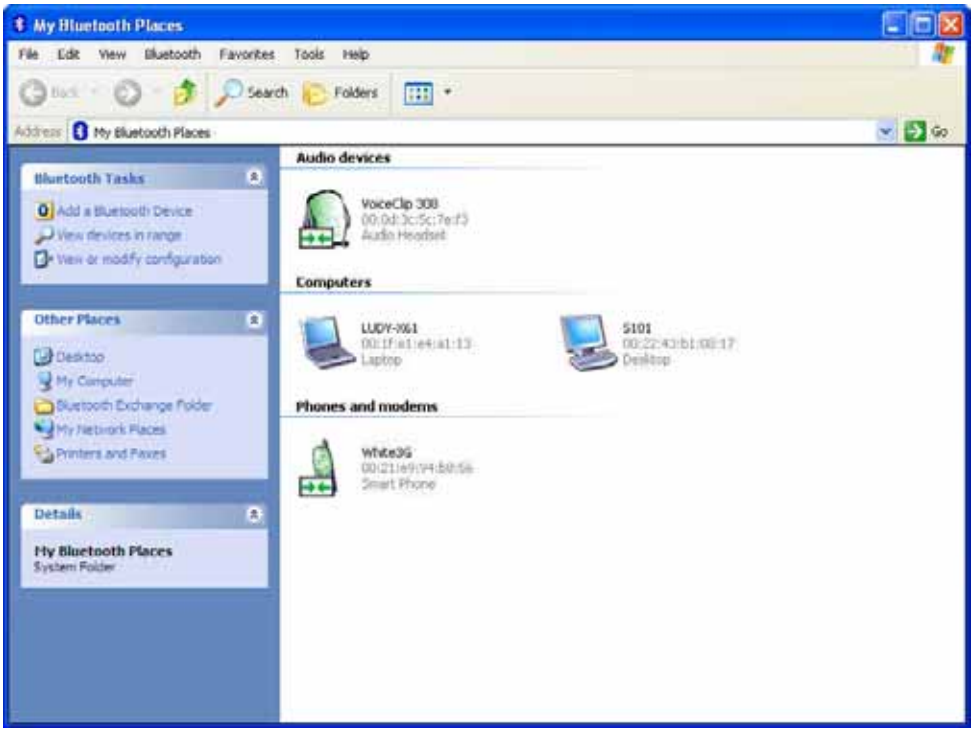

WIDCOMM Bluetooth Software
InstallShield Wizard Completed
The InstallShield Wizard has successfully installed WIDCOMM Bluetooth Software. Click Finish to exit the wizard.
Some of the Bluetooth functionality might not be available until the next time you log on.
< Back
Finish
Cancel

10. After the installation, a Bluetooth icon appears in the desktop menu, presenting the status of the BT-302USB adapter. To begin configuring the Bluetooth connection, right-click on the icon and select your prefer choice from the pop-up menu. To stop the configuration utility, right-click on the icon and click "**Stop the Bluetooth Device**"

2.1. Configuration Utility

The configuration utility is a powerful application that helps you configure you Bluetooth adapter with other Bluetooth embedded devices.
The utility appears as an icon in the system tray and on the desktop of Windows. You can open it by right-click the icon in the system tray and an options menu displays.

Explore My Bluetooth Places: Double-click the My Bluetooth Places icon on the desktop or right-click the Bluetooth icon in the system tray and select Explore My Bluetooth Places. It will show the Bluetooth devices that have been paired up before. You can easily re-connect the devices without going through the pairing process.

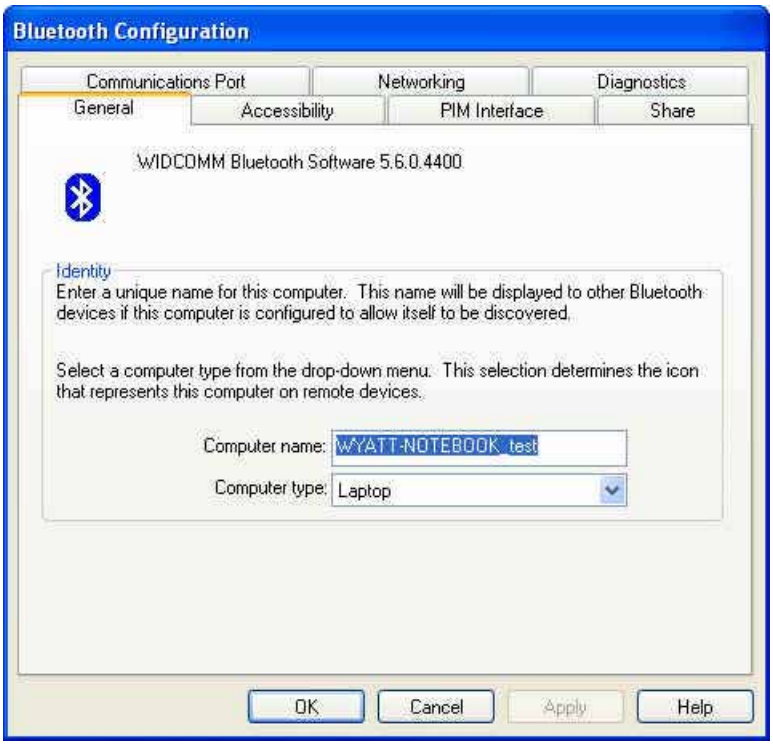


Add a Bluetooth Device: The Bluetooth Setup Wizard appears and it will help you with the following features:

- Configure how this computer accesses a service on another Bluetooth device
- Locate remote Bluetooth devices
- Configure the way that this computer provides services to remote Bluetooth devices
- Set the name and type of this Bluetooth device

Bluetooth Device Selection
Select a device
Remote devices must be in Discoverable mode for this computer to find them.
For assistance in making a remote device discoverable, refer to the user guide that came with the device.
LUDY-X61
S101
VoiceClip 308
White3G
Search Again
Show all devices
If the device you are looking for is not in the list, verify that the device has power and is operational. On some devices, you must press the Connect button to make the device discoverable.
< Back
Next >
Cancel

Bluetooth Configuration: The Bluetooth Configuration Panel provides access to settings for Bluetooth services, client applications, hardware, security, discovery, accessibility, default paths, event notification and other Bluetooth related items. To open the Bluetooth Configuration panel, right-click the Bluetooth icon in the system tray and select “Bluetooth Configuration”


Bluetooth Configuration
Communications Port
Networking
Diagnostics
General
Accessibility
PIM Interface
Share
WIDCOMM Bluetooth Software 5.6.0.4400
Identity
Enter a unique name for this computer. This name will be displayed to other Bluetooth devices if this computer is configured to allow itself to be discovered.
Select a computer type from the drop-down menu. This selection determines the icon that represents this computer on remote devices.
Computer name: WYATT-NOTEBOOK_test
Computer type: Laptop
OK
Cancel
Apply
Help

Bluetooth Devices: Quick access to the Bluetooth devices which were connected before. Right-click the Bluetooth icon in the system tray and select “Bluetooth Devices”

White3G
In Bluetooth Device Control, you can connect to and disconnect from device services and configure device settings.
Tasks
Synchronization settings
See also
Add a Bluetooth device
Show Bluetooth devices
Open Bluetooth settings
Help
Bluetooth Device Control
WYATT-NOTEBOOK_test
White3G
(Disconnected)
Phone Operations
Backup and Synchronization
Back up Contacts and Calendar from the (White3G) phone to this computer
Restore backed-up Contacts and Calendar to the (White3G) phone
Synchronize Contacts and Calendar between this computer and the (White3G) phone
Music and Audio
Play audio stored on the (White3G) phone through my computer
Connect
Personal Network and Communication
Join a personal area network
Connect

Start/Stop the Bluetooth Device: Start or Stop the Bluetooth service on this computer. If you select “Stop the Bluetooth Device,” all connection will be cut-off and the Bluetooth adapter will be disabled.

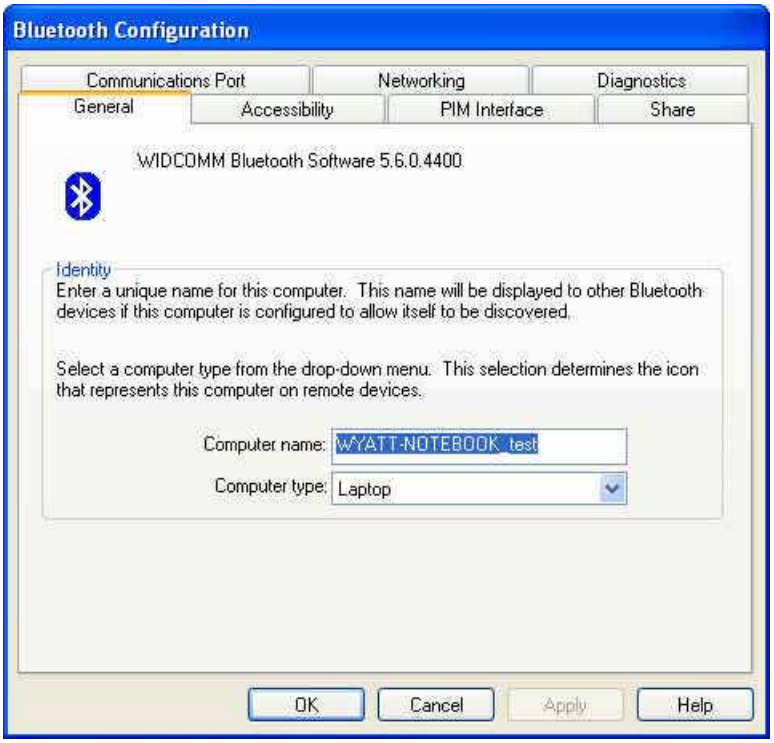
2.2. Bluetooth Configuration - General

General Configuration Settings

The settings on the General tab of the Bluetooth Configuration Panel determine the information that is displayed to the remote devices.

Computer name: enter a unique name to identify this computer to other Bluetooth devices nearby; this field cannot be left blank.

Computer type: select either Desktop or Laptop from the shortcut menu to set the type of icon remote devices will use to represent this computer.



2.3. Bluetooth Configuration - Accessibility

The Accessibility tab of the Bluetooth Configuration Panel lets you specify whether remote devices may access this computer, which remote devices have access, and whether an audio warning is played when a Personal Identification Number (PIN code) is required.

Allow other devices to discover this computer

Select “Let other Bluetooth devices discover this computer” to permit remote Bluetooth devices to find and report this computer.

Bluetooth Headsets

Enable “Control Skype calls using a hands-free device” allows you to talk on skype via Bluetooth headsets.

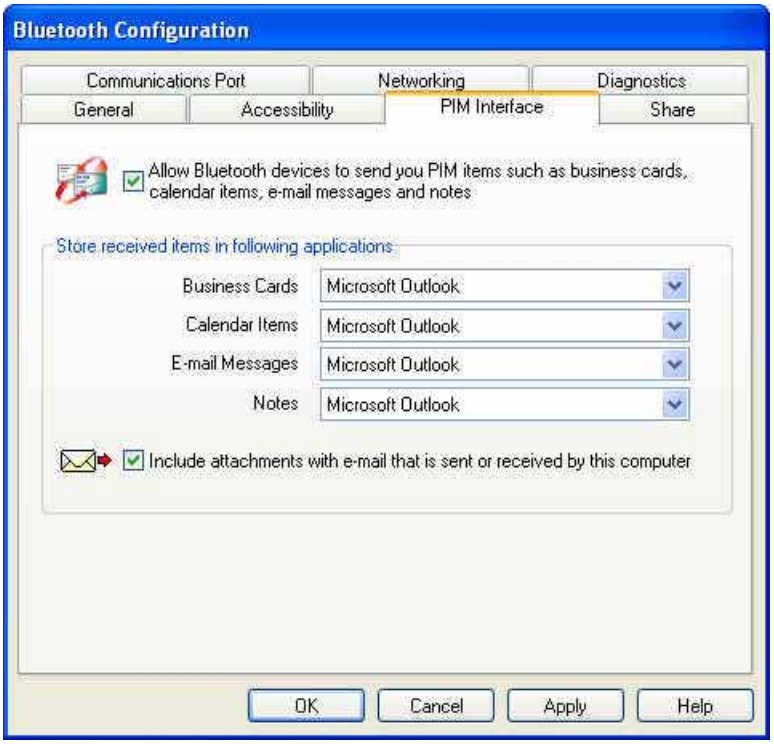
Notification

When a remote device connects to a service, there are three ways to setup the notification.

- Do not notify
- Use visual notification
- Use audio notification

2.4. Bluetooth Configuration – PIM Interface

The PIM Synchronization Application is used to synchronize the Personal Information Manager (PIM) database of this computer with the PIM database of a remote Bluetooth device.



Check or uncheck “Allow Bluetooth devices to send you PIM items such as business cards, calendar items, e-mail messages and notes” to enable/disable this function. The default setting is enabled.

The supported PIMs are listed below:

- Microsoft Outlook
- Microsoft Outlook Express
- Lotus Notes

The supported data types are listed below:

- Business cards
- Calendar items
- Email (with or without attachments)
- Notes

Check or uncheck “Include attachments with e-mail that is sent or received by this computer” to enable/disable this function. The default setting is enabled.

2.5. Bluetooth Configuration - Share

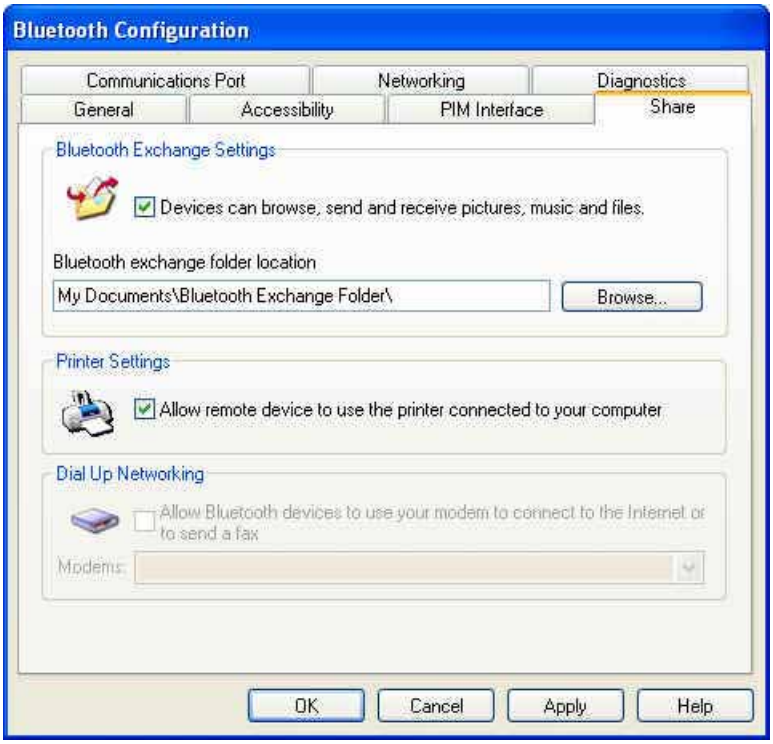
Bluetooth Exchange Settings

Check or uncheck “Devices can browse, send and receive pictures, music and files” to enable/disable this function. The default setting is enabled.

The default Bluetooth exchange folder is as listed below, you may change the location by click the “Browse” button.

My Documents\Bluetooth Exchange Folder

This is the highest-level directory on this computer to which a remote Bluetooth device has access. Devices that have been granted access to this computer’s Bluetooth Exchange Folder also have access to all sub-folders contained within that folder and all files in those sub-folders.



Printer Settings

Sharing your printer with remote Bluetooth devices by check or uncheck “Allow remote device to use the printer connected to your computer” to enable/disable this function. The default setting is enabled.

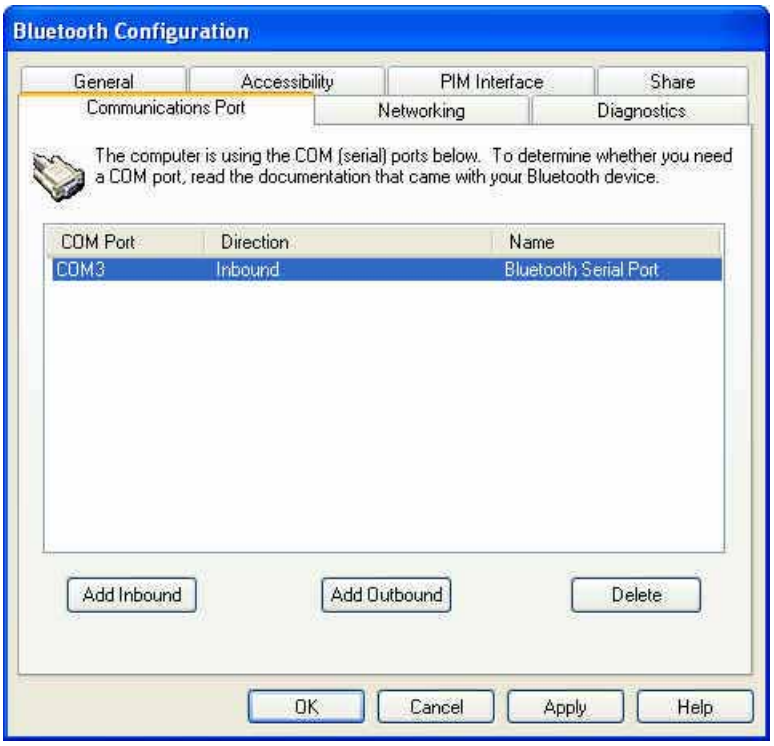
Dial Up Networking

The Bluetooth Dial-up Networking application allows this computer to use a modem that is physically connected to a remote device to access the Internet, log on to a remote network.

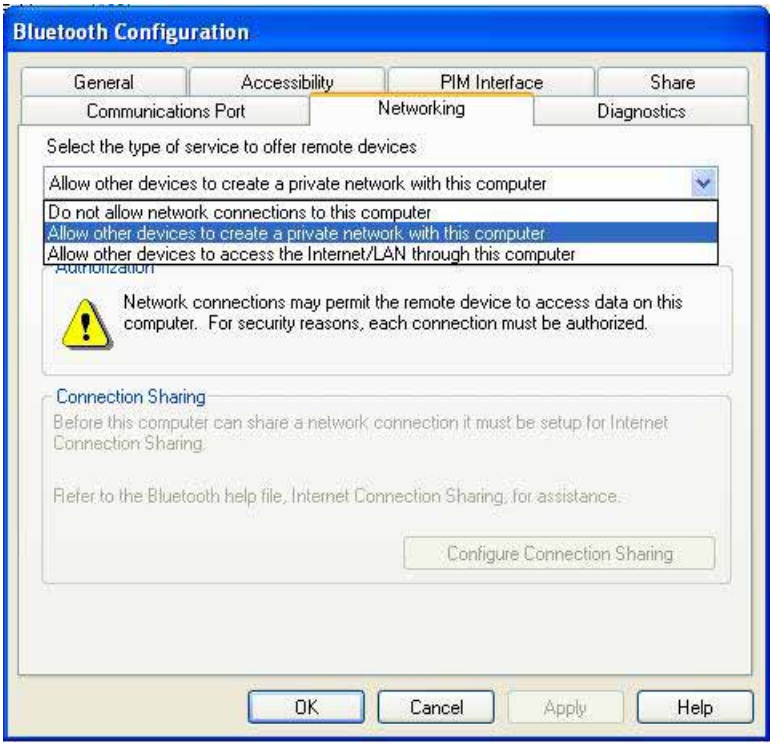
Check or uncheck “Allow Bluetooth devices to use your modem to connect to the Internet or to send a fax” to enable/disable this function. The default setting is disabled.

2.6. Bluetooth Configuration – Communications Port

The Bluetooth Serial Port application allows this computer to establish a wireless serial connection with a remote Bluetooth device. The applications on both this computer and the remote device must be configured to send and receive data to and from the respective communications port (COM port) assigned to the Bluetooth serial port. The wireless serial connection may then be used by the applications as though a physical serial cable connected the devices.



2.7. Bluetooth Configuration – Networking

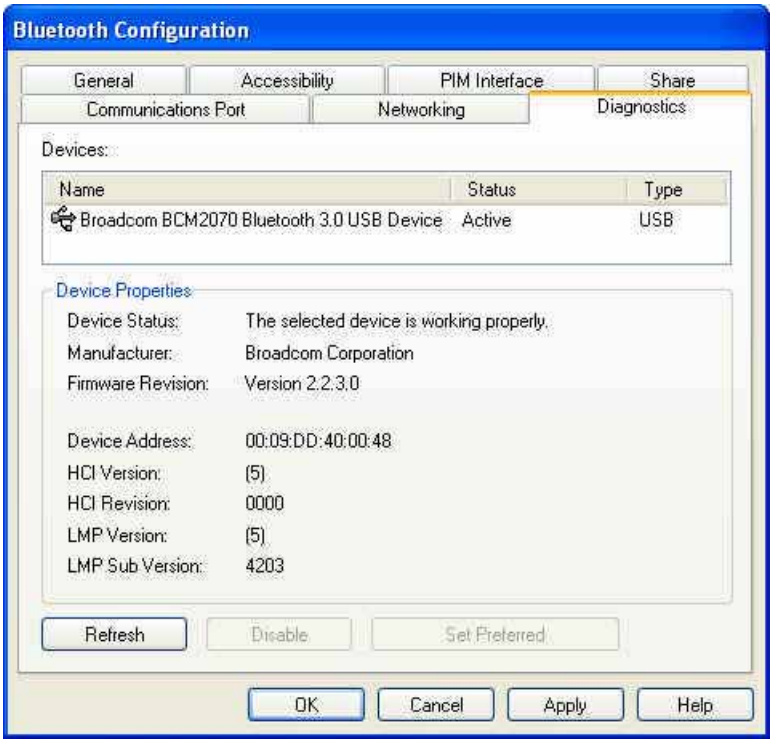

Bluetooth Configuration
General
Accessibility
PIM Interface
Share
Communications Port
Networking
Diagnostics
Select the type of service to offer remote devices
Allow other devices to create a private network with this computer
Do not allow network connections to this computer
Allow other devices to create a private network with this computer
Allow other devices to access the Internet/LAN through this computer
Network connections may permit the remote device to access data on this computer. For security reasons, each connection must be authorized.
Connection Sharing
Before this computer can share a network connection it must be setup for Internet Connection Sharing.
Refer to the Bluetooth help file, Internet Connection Sharing, for assistance.
Configure Connection Sharing
OK
Cancel
Apply
Help

The Bluetooth Network Access service makes it possible for a remote Bluetooth device to access a Local Area Network that is physically attached to this computer or allows a remote device to become part of an ad hoc network provided by this computer. After this computer has been configured to provide the Network Access service to other Bluetooth devices, it will not be able to use the Bluetooth Network Access service provided by another Bluetooth device without being re-configured. Put another way, this computer cannot be both a Bluetooth Network Access server and a Bluetooth Network Access client at the same time.

Select the type of service to offer remote devices:

- Do not allow network connections to this computer
- Allow other devices to create a private network with this computer
- Allow other devices to access the Internet/LAN through this computer

2.8. Bluetooth Configuration - Diagnostics



This page shows the general information about this Bluetooth adapter

Device Properties

Device Status: Showing whether the Bluetooth adapter is working properly or not

Manufacturer: Indicates the chipset manufacturer of this Bluetooth adapter

Firmware Revision: Showing the firmware version of this Bluetooth adapter

Device Address: The MAC address of this adapter

3 Specifications

Standards

• Bluetooh v3.0 (backward compatible with v1.1/1.2/2.0/2.1)

General

• Interface: USB 2.0, type A

• Chipset: Broadcom

• Frequency band: 2.4000 – 2.480 GHz

•Spread Spectrum: 79 Channel; FHSS (Frequency Hopping Spread Spectrum)

• Transfer Rates: 3Mbps

• Power Class: Class 2

• Receiving Sensitivity: -80dBm at 0.1% BER

• Antenna: Integrated Antenna

• Input Power: USB Bus Power

• Certification: FCC, CE

• LED: Power ON (blue)

• OS Support: Windows XP/Vista/7

Mac OS X 10.5/10.6

Size

• Dimensions: 4.5 (H) x 14.2 (W) x 19.3 (L) mm

• Weight: Approx 2.4g

Environmental

• Operating temperature: -10 ~ 50°C

• Storage temperature: -20 ~ 60°C (-4 ~ 14°F)

4 Wireless Network Glossary

The wireless network glossary contains explanation or information about common terms used in wireless networking products. Some of information in this glossary might be outdated, please use with caution.

802.11a
An IEEE specification for wireless networking that operates in the 5 GHz frequency range (5.15 GHz to 5.850 GHz) with a maximum of 54Mbps data transfer rate. The 5GHz frequency band is not as crowded as the 2.4GHz band. In addition, the 802.11a have 12 non-overlapping channels, comparing to 802.11b/g's 3 non-overlapping channels. This means the possibility to build larger non-interfering networks. However, the 802.11a deliver shorter distance at the same output power when comparing to 802.11g.

802.11b
International standard for wireless networking that operates in the 2.4GHz frequency band (2.4 GHz to 2.4835 GHz) and provides a throughput up to 11 Mbps.

802.11d
Also known as “Global Roaming”. 802.11d is a standard for use in countries where systems using other standards in the 802.11 family are not allowed to operate.

802.11e
The IEEE QoS standard for prioritizing traffic of the VoIP and multimedia applications. The WMM is based on a subset of the 802.11e.

802.11g

A standard provides a throughput up to 54 Mbps using OFDM technology. It also operates in the 2.4GHz frequency band as 802.11b. 802.11g devices are backward compatible with 802.11b devices.

802.11h

This IEEE standard define the TPC (transmission power control) and DFS (dynamic frequency selection) required to operate WiFi devices in 5GHz for EU.

802.11i

The IEEE standard for wireless security, 802.11i standard includes TKIP, CCMP, and AES encryption to improve wireless security. It is also know as WPA2.

802.11n

802.11n is a recent amendment which improves upon the previous 802.11 standards by adding multiple-input multiple-output (MIMO) and many other newer features. The IEEE has approved the amendment and it was published in October 2009. Enterprises, however, have already begun migrating to 802.11n networks based on the Wi-Fi Alliance's certification of products conforming to a 2007 draft of the 802.11n proposal. 802.11n provides a throughput up to 300Mbps using OFDM technology.

802.3ad

802.3ad is an IEEE standard for bonding or aggregating multiple Ethernet ports into one virtual port (also known as trunking) to increase the bandwidth.

802.3af

This is the PoE (Power over Ethernet) standard by IEEE committee. 803.af uses 48V POE standard that can deliver up to 100 meter distance over Ethernet cable.

802.1d STP

Spanning Tree Protocol. It is an algorithm to prevent network from forming. The STP protocol allows net work to provide a redundant link in the event of a link failure. It is advise to turn on this option for multi-link bridge network.

802.1Q Tag VLAN

In 802.1Q VLAN, the VLAN information is written into the Ethernet packet itself. Each packet carries a VLAN ID (called Tag) as it traveled across the network. Therefore, the VLAN configuration can be configured across multiple switches. In 802.1Q spec, possible 4096 VLAN ID can be created. Although for some devices, they can only view in frames of 256 ID at a time.

802.1x

802.1x is a security standard for wired and wireless LANs. In the 802.1x parlance, there are usually supplicants (client), authenticator (switch or AP), and authentication server (radius server) in the network. When a supplicants request a service, the authenticator will pass the request and wait for the authentication server to grant access and register accounting. The 802.1x is the most widely used method of authentication by WISP.

Ad-hoc

A Peer-to-Peer wireless network. An Ad-hoc wireless network do not use wireless AP or router as the central hub of the network. Instead, wireless client are connected directly to each other. The disadvantage of Adhoc network is the lack of wired interface to Internet connections. It is not recommended for network more than 2 nodes.

Access Point (AP)

The central hub of a wireless LAN network. Access Points have one or more Ethernet ports that can connect devices (such as Internet connection) for sharing. Multi-function Access Point can also function as an Ethernet client, wireless bridge, or repeat signals from other AP. Access Points typically have more wireless functions comparing to wireless routers.

ACK Timeout

Acknowledgement Timeout Windows. When a packet is sent out from one wireless station to the other, it will waits for an Acknowledgement frame from the remote station. The station will only wait for a certain amount of time; this time is called the ACK timeout. If the ACK is NOT received within that timeout period then the packet will be re-transmitted resulting in reduced throughput. If the ACK setting is too high then throughput will be lost due to waiting for the ACK Window to timeout on lost packets. If the ACK setting is too low then the ACK window will have expired and the returning packet will be dropped, greatly lowering throughput. By having the ability to adjust the ACK setting we can effectively optimize the throughput over long distance links. This is especially true for 802.11a and 802.11g networks. Setting the correct ACK timeout value needs to consider 3 factors: distance, AP response time, and interference.

Bandwidth Management

Bandwidth Management controls the transmission speed of a port, user, IP address, and application. Router can use bandwidth control to limit the Internet connection speed of individual IP or Application. It can also guarantee the speed of certain special application or privileged IP address - a crucial feature of QoS (Quality of Service) function.

Bootloader

Bootloader is the under layering program that will start at the power-up before the device loads firmware. It is similar to BIOS on a personal computer. When a firmware crashed, you might be able to recover your device from bootloader.

Bridge

A product that connects 2 different networks that uses the same protocol. Wireless bridges are commonly used to link network across remote buildings. For wireless application, there are 2 types of Bridges. WDS Bridge can be used in Point-to-Point or Point-to-Multipoint topology. Bridge Infrastructure works with AP mode to form a star topology.

Cable and Connector Loss

During wireless design and deployment, it is important to factor in the cable and connector loss. Cable and connector loss will reduce the output power and receiver sensitivity of the radio at connector end. The longer the cable length is, the more the cable loss. Cable loss should be subtracted from the total output power during distance calculation. For example, if the cable and connector loss is 3dBm and the output power is 20dBm; the output power at the cable end is only 17dBm.

Client

Client means a network device or utility that receives service from host or server. A client device means end user device such as wireless cards or wireless CPE.

CPE Devices

CPE stands for Customer Premises Equipment. A CPE is a device installed on the end user's side to receive network services. For example, on an ADSL network, the ADSL modem/router on the subscriber's home is the CPE device. Wireless CPE means a complete Wireless (usually an AP with built-in Antenna) that receives wireless broadband access from the WISP. The opposite of CPE is CO.

CTS

Clear To Send. A signal sent by a device to indicate that it is ready to receive data.

DDNS

Dynamic Domain Name System. An algorithm that allows the use of dynamic IP address for hosting Internet Server. A DDNS service provides each user account with a domain name. A router with DDNS capability has a built-in DDNS client that updates the IP address information to DDNS service provider whenever there is a change. Therefore, users can build website or other Internet servers even if they don't have fixed IP connection.

DHCP

Dynamic Hosting Configuration Protocol. A protocol that enables a server to dynamically assign IP addresses. When DHCP is used, whenever a computer logs onto the network, it automatically gets an IP address assigned to it by DHCP server. A DHCP server can either be a designated PC on the network or another network device, such as a router.

DMZ

Demilitarized Zone. When a router opens a DMZ port to an internal network device, it opens all the TCP/UDP service ports to this particular device. The feature is used commonly for setting up H.323 VoIP or Multi-Media servers.

DNS

A program that translates URLs to IP addresses by accessing a database maintained on a collection of Internet servers.

Domain Name

The unique name that identifies an Internet site. Domain Names always have 2 or more parts, separated by dots. In www.airlive.com, the "airlive.com" is the doman name.

DoS Attack

Denial of Service. A type of network attack that floods the network with useless traffic. Many DoS attacks, such as the Ping of Death and Teardrop attacks, exploit limitations in the TCP/IP protocols.

Encryption

Encoding data to prevent it from being read by unauthorized people. The common wireless encryption schemes are WEP, WPA, and WPA2.

ESSID (SSID)

The identification name of an 802.11 wireless network. Since wireless network has no physical boundary liked wired Ethernet network, wireless LAN needs an identifier to distinguish one network from the other. Wireless clients must know the SSID in order to associate with a WLAN network. Hide SSID feature disable SSID broadcast, so users must know the correct SSID in order to join a wireless network.

Firewall

A system that secures a network and prevents access by unauthorized users. Firewalls can be software, router, or gateway. Firewalls can prevent unrestricted access into a network, as well as restricting data from flowing out of a network.

Firmware

The program that runs inside embedded device such as router or AP. Many network devices are firmware upgradeable through web interface or utility program.

FTP

File Transfer Protocol. A standard protocol for sending files between computers over a TCP/IP network and the Internet.

Fragment Threshold

Frame Size larger than this will be divided into smaller fragment. If there are interferences in your area, lower this value can improve the performance. If there are not, keep this parameter at higher value. The default size is 2346. You can try 1500, 1000, or 500 when there are interference around your network.

Full Duplex

The ability of a networking device to receive and transmit data simultaneously. In wireless environment, this is usually done with 2 or more radios doing load balancing.

Gateway

In the global Internet network, the gateways are core routers that connect networks in different IP subnet together. In a LAN environment with an IP sharing router, the gateway is the router. In an office environment, gateway typically is a multi-function device that integrates NAT, firewall, bandwidth management, and other security functions.

Hotspot

A place where you can access Wi-Fi service. The term hotspot has two meanings in wireless deployment. One is the wireless infrastructure deployment, the other is the Internet access billing system. In a hotspot system, a service provider typically need an authentication and account system for billing purposes, and a wireless AP network to provide access for customers.

IGMP Snooping

Internet Group Management Protocol (IGMP) is a Layer 3 protocol to report IP multicast memberships to neighboring multicast switches and routers. IGMP snooping is a feature that allows an Ethernet switch to "listen in" on the IGMP conversation between hosts and routers. A switch support IGMP snooping has the possibility to avoid multicast traffic being treated as broadcast traffic; therefore, reducing the overall traffic on the network.

Infrastructure Mode

A wireless network that is built around one or more access points to provide wireless clients access to wired LAN / Internet service. The opposite of Infrastructure mode is Ad-hoc mode.

IP address

IP (Internet Protocol) is a layer-3 network protocol that is the basis of all Internet communication. An IP address is 32-bit number that identifies each sender or receiver of information that is sent across the Internet. An IP address has two parts: an identifier of a particular network on the Internet and an identifier of the particular device (which can be a server or a workstation) within that network. The new IPv6 specification supports 128-bit IP address format.

IPsec

IP Security. A set of protocols developed by the IETF to support secure exchange of packets at the IP layer. IPsec has been deployed widely to implement Virtual Private Networks (VPNs). IPsec supports two encryption modes: Transport and Tunnel. Transport mode encrypts only the data of each packet, but leaves the header untouched. The more secure Tunnel mode encrypts both the header and the payload. On the receiving side, an IPSec-compliant device decrypts each packet.

LACP (802.3ad) Trunking

The 802.3ad Link Aggregation standard defines how to combine the several Ethernet ports into one high-bandwidth port to increase the transmission speed. It is also known as port trunking. Both device must set the trunking feature to work.

MAC (Media Access Control)

MAC address provides layer-2 identification for Networking Devices. Each Ethernet device has its own unique address. The first 6 digits are unique for each manufacturer. When a network device have MAC access control feature, only the devices with the approved MAC address can connect with the network.

Mbps (Megabits per Second)
One million bits per second; a unit of measurement for data transmission

MESH
Mesh is an outdoor wireless technology that uses Spanning Tree Protocol (STP) and Wireless Distribution system to achieve self-forming, self-healing, and self-configuring outdoor network. MESH network are able to take the shortest path to a destination that does not have to be in the line of site.

MIMO (Multi-Input-Multi-Output)
A Smart Antenna technology designed to increase the coverage and performance of a WLAN network. In a MIMO device, 2 or more antennas are used to increase the receiver sensitivity and to focus available power at intended Rx.

NAT (Network Address Translation)
A network algorithm used by Routers to enables several PCs to share single IP address provided by the ISP. The IP that a router gets from the ISP side is called Real IP, the IP assigned to PC under the NAT environment is called Private IP.

Node
A network connection end point, typically a computer.

Packet
A unit of data sent over a network.

Passphrase
Used much like a password, a passphrase simplifies the WEP encryption process by automatically generating the WEP encryption keys for the company products.

POE (Power over Ethernet)

A standard to deliver both power and data through one single Ethernet cable (UTP/STP). It allows network device to be installed far away from power ource. A PoE system typically compose of 2 main component: DC Injector (Base Unit) and Splitter(Terminal Unit). The DC injector combines the power and data, and the splitter separates the data and power back. A PoE Access Point or CPE has the splitter built-in to the device. The IEEE 802.3af is a POE spec that uses 48 volt to deliver power up to 100 meter distance.

Port

This word has 2 different meaning for networking.
The hardware connection point on a computer or networking device used for plugging in a cable or an adapter.
The virtual connection point through which a computer uses a specific application on a server.

PPPoE

Point-to- Point Protocol over Ethernet. PPPoE relies on two widely accepted standards: PPP and Ethernet. PPPoE is a specification for connecting the users on an Ethernet to the Internet through a common broadband medium, such as a single DSL line, wireless device or cable modem.

PPTP

Point-to-Point Tunneling Protocol: A VPN protocol developed by PPTP Forum. With PPTP, users can dial in to their corporate network via the Internet. If users require data encryption when using the Windows PPTP client, the remote VPN server must support MPPE (Microsoft Point-To-Point Encryption Protocol) encryption. PPTP is also used by some ISP for user authentication, particularly when pairing with legacy Alcatel / Thomson ADSL modem.

Preamble Type

Preamble are sent with each wireless packet transmit for transmission status. Use the long preamble type for better compatibility. Use the short preamble type for better performance

Rate Control

Ethernet switches' function to control the upstream and downstream speed of an individual port. Rate Control management uses "Flow Control" to limit the speed of a port. Therefore, the Ethernet adapter must also have the flow control enabled. One way to force the adapter's flow control on is to set a port to half-duplex mode.

RADIUS (Remote Authentication Dial-In User Service)

An authentication and accounting system used by many Internet Service Providers (ISPs). When you dial in to the ISP, you must enter your username and password. This information is passed to a RADIUS server, which checks that the information is correct, and then authorizes access to the ISP system. Radius typically uses port 1812 and port 1813 for authentication and accounting port. Though not an official standard, the RADIUS specification is maintained by a working group of the IETF.

Receiver Sensitivity

Receiver sensitivity means how sensitive is the radio for receiving signal. In general; the slower the transmission speed, the more sensitive the radio is. The unit for Receiver Sensitivity is in dB; the lower the absolute value is, the higher the signal strength. For example, -50dB is higher than -80dB.

RJ-45

Standard connectors for Twisted Pair copper cable used in Ethernet networks. Although they look similar to standard RJ-11 telephone connectors, RJ-45 connectors can have up to eight wires, whereas telephone connectors have only four.

Router

An IP sharing router is a device that allows multiple PCs to share one single broadband connection using NAT technology. A wireless router is a device that combines the functions of wireless Access Point and the IP sharing router.

RSSI

Receiver Sensitivity Index. RSSI is a value to show the Receiver Sensitivity of the remote wireless device. In general, remote APs with stronger signal will display higher RSSI values. For RSSI value, the smaller the absolute value is, the stronger the signal. For example, “-50db” has stronger signal than “-80dB”. For outdoor connection, signal stronger than -60dB is considered as a good connection.

RTS

Request To Send. A packet sent when a computer has data to transmit. The computer will wait for a CTS (Clear To Send) message before sending data.

RTS Threshold

RTS (Request to Send). The RTS/CTS(clear to send) packet will be send before a frame if the packet frame is larger than this value. Lower this value can improve the performance if there are many clients in your network. You can try 1500, 1000 or 500 when there are many clients in your AP’s network.

SNMP (Simple Network Management Protocol)

A set of protocols for managing complex networks. The SNMP network contains 3 key elements: managed devices, agents, and network-management systems (NMSs). Managed devices are network devices that content SNMP agents. SNMP agents are programs that reside SNMP capable device's firmware to provide SNMP configuration service. The NMS typically is a PC based software such as HP Openview that can view and manage SNMP network device remotely.

SSH

Developed by SSH Communications Security Ltd., Secure Shell is a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over insecure channels. It is a replacement for rlogin, rsh, rcp, and rdist.

SSL

Secure Sockets Layer. It is a popular encryption scheme used by many online retail and banking sites to protect the financial integrity of transactions. When an SSL session begins, the server sends its public key to the browser. The browser then sends a randomly generated secret key back to the server in order to have a secret key exchange for that session. SSL VPN is also known as Web VPN. The HTTPS and SSH management interface use SSL for data encryption.

Subnet Mask

An address code mask that determines the size of the network. An IP subnet are determined by performing a BIT-wise AND operation between the IP address and the subnet mask. By changing the subnet mask, you can change the scope and size of a network.

Subnetwork or Subnet

Found in larger networks, these smaller networks are used to simplify addressing between numerous computers. Subnets connect to the central network through a router, hub or gateway. Each individual wireless LAN will probably use the same subnet for all the local computers it talks to.

Super A

Super A is an Atheros proprietary turbo mode to increase speed over standard 802.11a mode. It adds Bursting and Compression to increase the speed. If you live in countries that prohibit the channel binding technology (i.e. Europe), you should choose “Super-A without Turbo) if you need more speed than 11a mode

TCP

A layer-4 protocol used along with the IP to send data between computers over the Internet. While IP takes care of handling the actual delivery of the data, TCP takes care of keeping track of the packets that a message is divided into for efficient routing through the Internet.

Turbo A

Turbo A is an Atheros proprietary turbo mode to increase speed over standard 802.11a mode. It uses channel binding technology to increase speed. There are 2 types of Turbo A modes: Dynamic Turbo and Static Turbo. In Dynamic Turbo, the channel binding will be used only if necessary. In Static Turbo, the channel binding is always on. This protocol may be combined with Super-A model to increase the performance even more. The used of channel binding might be prohibited in EU countries.

TX Output Power

Transmit Output Power. The TX output power means the transmission output power of the radio. Normally, the TX output power level limit for 2.4GHz 11g/b is 20dBm at the antenna end. The output power limit for 5GHz 802.11a is 30dBm at the antenna end.

UDP (User Datagram Protocol)

A layer-4 network protocol for transmitting data which does not require acknowledgement from the recipient of the data.

Upgrade

To replace existing software or firmware with a newer version.

Upload
To send a file to the Internet or network device.

URL (Uniform Resource Locator)
The address of a file located on the Internet.

VPN (Virtual Private Network)
A type of technology designed to increase the security of information transferred over the Internet. VPN creates a private encrypted tunnel from the end user's computer, through the local wireless network, through the Internet, all the way to the corporate network.

Walled Garden
On the Internet, a walled garden refers to a browsing environment that controls the information and Web sites the user is able to access. This is a popular method used by ISPs in order to keep the user navigating only specific areas of the Web

WAN (Wide Area Network)
A communication system of connecting PCs and other computing devices across a large local, regional, national or international geographic area. A WAN port on the network device means the port (or wireless connection) that is connected to the Internet side of the network topology.

WEP (Wired Equivalent Privacy)
A wireless encryption protocol. WEP is available in 40-bit (64-bit), 108-bit (128-bit) or 152-bit (Atheros proprietary) encryption modes.

WPA (Wi-Fi Protected Access)

It is an encryption standard proposed by WiFi for advance protection by utilizing a password key (TKIP) or certificate. It is more secure than WEP encryption. The WPA-PSK utilizes pre-share key for encryption/authentication.

WPA2 (Wi-Fi Protected Access 2)

WPA2 is also known as 802.11i. It improves on the WPA security with CCMP and AES encryption. The WPA2 is backward compatible with WPA. WPA2-PSK utilizes pre-share key for encryption/authentication.

Wi-Fi (Wireless Fidelity)

An interoperability certification for wireless local area network (LAN) products based on the IEEE 802.11 standards. The governing body for Wi-Fi is called Wi-Fi Alliance (also known as WECA).

WiMAX (Worldwide Interoperability for Microwave Access)

A Wireless Metropolitan Network technology that complies with IEEE 802.16 and ETSI Hiperman standards. The orginal 802.16 standard call for operating frequency of 10 to 66Ghz spectrum. The 802.16a amendment extends the original standard into spectrum between 2 and 11 Ghz. 802.16d increase data rates to between 40 and 70 Mbps/s and add support for MIMO antennas, QoS, and multiple polling technologies. 802.16e adds mobility features, narrower bandwidth (a max of 5 mhz), slower speed and smaller antennas. Mobility is allowed up to 40 mph.

WDS (Wireless Distribution System)

WDS defines how multiple wireless Access Point or Wireless Router can connect together to form one single wireless network without using wired uplinks. WDS associate each other by MAC address, each device

WLAN (Wireless Local Area Network)

A type of local-area network that uses high-frequency radio waves rather than wires to communicate between nodes. The most popular standard for WLAN is the 802.11 standards.

WMM (Wi-Fi Multimedia)

WMM is a standard to prioritize traffic for multimedia applications. The WMM prioritize traffic\ on Voice-over-IP (VoIP), audio, video, and streaming media as well as traditional IP data over the AP.

WMS (Wireless Management System)

An utility program to manage multiple wireless AP/Bridges.